PATENT

REMARKS

Reconsideration of the rejections set forth in the Office action dated 6/30/2005 is respectfully requested under the provisions of 37 CFR §1.111(b).

Claims 1-19 are pending.

Claims 1-19 stand rejected.

No claims were amended.

Paragraphs [0003]-[0005] were amended to insert application serial numbers for the related applications. No new matter was added.

Applicant hereby petitions for a two month extension of time and authorizes the charging of any necessary fees, other than the issue fee, to Xerox Corporation Deposit Account No. 24-0025.

I. Rejections under 35 USC §102(e)

Claims 1-19 are rejected under 35 U.S.C. 102(e) as being anticipated by Lowensohn et al. (U.S.Pub-20040230809).

A prima facie case of anticipation is established when the Examiner provides a single reference that teaches or enables each of the claimed elements (arranged as in the claim) expressly or inherently as interpreted by one of ordinary skill in the art.

Applicant respectfully traverses this rejection to the claims as a prima facie case has not been established.

Lowensohn teaches technology related to a wireless badge that can be provisioned using techniques that were well known at the time of the instant invention. For example, data to be stored in the badge "must be encrypted prior to writing to the BARB Badge 100 (and decrypted after reading from the BARB Badge 100)" (sec: [0270], also see [0159], [0162], [0236], and [0238]). Applications that read this data from the badge must obtain the crypto key for that badge to access the data [0143], [0206], [0236].

10/656551   Page 7 of 13   A3162Q-US-NP

PAGE 9/15 * RCVD AT 11/23/2005 9:09:37 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/26 * DNIS:2738300 * CSID:+6508124274 * DURATION (mm-ss):03-54

PATENT

In addition, the badge can include on-board encryption capability ([0057], [0259]). However, Lowensohn does not provide any detail on how the on-board encryption capability securely receives its key other than paragraphs [0270]-[0271] that describe well known techniques for providing a Key using a secure channel (see: last sentence of paragraph [0271]).

Lowensohn recognizes the potential security problems with IR and RF transmissions and teaches using a strong encryption algorithm for these transmissions [0057].

Lowensohn's badges are recognized by base stations that obtain the encrypted data from the badge and makes this encrypted data available to system applications. The system applications must first obtain a key to decode the encrypted data received from the badge to perform the application's function.

Lowensohn does not teach the use of a preferred channel as is claimed by the original independent claims of the instant application. Lowensohn does not teach the provisioning of a wireless device over a preferred channel, or of automatically configuring the wireless device, responsive to the provisioning, to communicate over a secure communication channel. Applicant believes this will become clear from the following discussion.

Summary of the technology disclosed by the instant application

One problem addressed by the claimed invention simplifies the incredibly difficult and complex creation and management of PKIs and distribution of certificates. This cost of setting up a PKI keeps individuals from considering larger-scale use of public key cryptography in embedded devices (e.g. cell phones, printers, etc), as each of these devices would have to be "provisioned" with a certificate before use. Furthermore, the key management and distribution problem described above in the PKI context exists with any secure credential infrastructure that uses a credential issuing authority to issue credentials. Furthermore, wireless networks have proved notoriously difficult for even knowledgeable corporate IT departments to securely configure. This has led to many deployed networks exposing information and network resources to strangers thus, leaving

PATENT

client machines vulnerable to attack. It is difficult, if not impossible, for network users to effectively configure and manage these wireless networks to make them secure. (see: [0011]-[0013]).

The claimed invention allows a device to obtain provisioning information from a provisioning device over a preferred channel and to automatically configure the device, responsive to the provisioning information received over the preferred channel, such that the device can send data over a secure communication channel. The provisioning can be (for example) of a certificate, or parameters to setup a wireless device for secure transmissions.

The preferred channel is explained within the specification to use "a location-limited channel or any other channel that has both a demonstrative identification property and an authenticity property".

The preferred channel uses communication technologies that have inherent physical limitations on their transmissions (for example, short range communication, use of visible light etc.). The *authenticity property* means that it is impossible or difficult for an attacker to transmit over the preferred channel or tamper with messages sent over the preferred channel without detection by the legitimate parties to the communication (attack detection only requires that the human participants know the number of the participants (devices) that are communicating over the preferred channel).

The *demonstrative identification property* of the preferred channel means that human operators are aware of which devices are communicating with each other over the preferred channel and that the human operators can easily detect when an attack is being made on the preferred channel.

It is important to realize that the preferred channel does not require secrecy (that is, an attacker can monitor the transmissions on the preferred channel) so long as the attacker cannot transmit on the preferred channel without detection. By using the preferred channel to pre-authenticate the keys (and to provide any provisioning information) that will be sent to the wireless sensor, the administrator of the secure credential infrastructure is assured that keys are only provided to wireless sensors that

PATENT

have had access to the preferred channel. Thus, establishing "trust" because the user of the wireless sensor must have had physical access to the preferred channel used by the provisioning device. Once "trust" is established, conventional security establishment techniques can be used to establish a secured channel with the wireless sensor. This allows the wireless sensor to communicate over a secure communication channel.

One example of the technology is that of providing simple administration of a PKI. If the provisioning device is within an access-controlled building, then a person who is able to obtain legal access to the provisioning device within the building is trusted. That trusted person can place their computer (or wireless sensor) in proximity to the provisioning device (where the preferred channel is a location limited channel), and have that computer (or wireless sensor) automatically provisioned for membership in the PKI.

Analysis of the Claims in light of Lowensohn

Looking now to original independent claims 1, 7 and 13: The invention of original claim 1 is directed to a computer controlled method comprising:

establishing communication between a wireless sensor and a provisioning device over a **preferred channel**;

receiving provisioning information from said provisioning device over said preferred channel; and

automatically configuring said wireless sensor for transmitting sensor information over a secure communication channel **responsive to said provisioning information**.

Applicant admits that one skilled in the art at the time of the invention would understand the use of public and private keys, and PKI infrastructures.

As is well known, and as recently restated by US Court of Appeals for the Federal Circuit in Phillips v. AWH Corporation that was decided on July 12, 2005, the inventor can be their own lexicographer. The claims must be read in view of the specification, of which they are a part. The specification is the primary basis for construing the claims.

PATENT

The specification may reveal a special definition given to a claim term by the patentee that differs from the meaning it would otherwise possess. In such cases, the inventor's lexicography governs. The "ordinary meaning" of a claim term is its meaning to the ordinary artisan after reading.the entire patent.

The preferred channel is explained within the specification to use "a location-limited channel or any other channel that has both a demonstrative identification property and an authenticity property" (see [0051]). The demonstrative identification property is described at paragraph [0052] and the authenticity property is described at paragraphs [0053] and [0054]. The consequence of the use of the preferred channel is described at paragraph [0055].

Applicant believes it is likely the Examiner was not fully aware of the meaning of the term "preferred channel" as having both a demonstrative identification property and an authenticity property.

Nothing in Lowensohn teaches a "preferred channel" as that term would be understood by one skilled in the art after reading the entire patent. While Lowensohn uses location limited communication (IR and RF) technologies, these communications are not over a preferred channel. Communication is either completely secure (such as is the case where Lowensohn's badges have encryption capability and the key for the secure communication has been provided using known technology), or the data communicated from the badge was encrypted prior to being stored in the badge. Nothing in Lowensohn teaches sending public information across an open channel that has the authenticity property and the demonstrative identification property. Lowensohn assumes that "trust" has already been established between the provisioning devices (by asserting that the badge has the capability to encrypt communications) or that no trust has been established (hence the need to encrypt the data stored on the badges).

The Office Action cited Lowensohn's Fig. 1 and paragraph [0037] as teaching "establishing communication between a wireless sensor and a provisioning device over a preferred channel". Fig. 1 and accompanying text teaches a badge in communication with a base station that communicates with a computer. The badge-base station

PATENT

communication being a **secure** IR or RF communication [0037]. The preferred channel of the instant invention is not a secure channel in that it does not require secrecy [0054]. That is, data is provided via the preferred channel and the information contained in the data can be monitored by an attacker. Because Lowensohn's IR and RF channels are secure, Lowensohn does not teach the preferred channel of the instant invention.

The Office Action cited Lowensohn's Fig.1, and paragraphs [0009]-[0010] and [0039]-[0040] as teaching "receiving provisioning information from said provisioning device over said preferred channel". The cited paragraphs all teach the use of secure communications or encrypted data between the badge and the badge-base station and/or computer-based system. As discussed above, Lowensohn does not teach a "preferred channel" as that term would be understood by one skilled in the art after reading the entire patent. Thus, these references do not teach receiving provisioning information over the preferred channel.

The Office Action cited Lowensohn's Figs.1 and 4, and paragraphs [0009]-[0010], [0059] as teaching "automatically configuring said wireless sensor for transmitting sensor information over a secure communication channel responsive to said provisioning information". [0059] teaches use of a well known PKI for distributing credentials and determining "trust" between devices. This reference also does not teach the "preferred channel". Nor does Lowensohn teach automatically configuring the wireless sensor responsive to the provisioning information provided over the location limited channel.

Thus, Lowensohn does not teach or enable each of the claimed elements (arranged as in the claim) expressly or inherently as interpreted by one of ordinary skill in the art. For this reason, Applicant respectfully traverses this rejection of **original claim 1**. Original independent claim 7 is a program product claim having scope similar to original claim 1. Original independent claim 13 is an apparatus claim having scope similar to original claim 1. Thus, for the previously presented reasons, Applicant respectfully traverses this rejection to **original claims 7 and 13**.

PATENT

Original claims 2-6, 8-12, and 14-19 depend on and further limit (directly or through intervening dependent claims) their respective independent claims. Thus, applicant respectfully traverses the rejection to these claims.

Since all rejections, objections and requirements contained in the outstanding official action have been fully answered or traversed and shown to be inapplicable to the present claims, it is respectfully submitted that reconsideration is now in order under the provisions of 37 CFR §1.111(b) and such reconsideration is respectfully requested. Upon reconsideration, it is also respectfully submitted that this application is in condition for allowance and such action is therefore respectfully requested.

The undersigned Xerox Corporation attorney hereby authorizes the charging of any necessary fees, other than the issue fee, to Xerox Corporation Deposit Account No. 24-0025. This also constitutes a request for any needed extension of time and authorization to charge all fees therefor to Xerox Corporation Deposit Account No. 24-0025.

Should any additional issues remain, or if I can be of any additional assistance, please do not hesitate to contact me at (650) 812-4259.

Respectfully submitted,

DANIEL B. CURTIS
Attorney for Applicants
Reg. No. 39,159
(650) 812-4259
dbcurtis@parc.com